CLAIMS

What is claimed is:

1.   A method of authenticating a client, the method comprising:

receiving a record ID for a user, and a one-time key generated by the

server and encrypted with a user's public key by the server;

receiving the user's authentication data from the client;

determining if the user's authentication data matches the record ID; and

if so, decrypting the one-time key with the user's private key, and

returning the decrypted one-time key to the client.

2.   The method of claim 1, further comprising registering the user,

registering comprising:

receiving a registration authentication data from the user;

generating a random public key/private key pair for the user;

generating a random record ID for the user; and

associating the authentication data and the private key with the record ID.

3.   The method of claim 2, further comprising:

sending the record ID and the public key to the user.

4.   The method of claim 2, further comprising establishing a secure

connection with the user prior to receiving registration authentication data.

1   5.   The method of claim 1, wherein a web page presented by the server

2   to the client prompts the user to enter the authentication data to log in to the

3   server.

1   6.   The method of claim 5, wherein the client's authentication data is

2   automatically redirected to the authentication server.

1   7.   The method of claim 1, wherein the authentication data is biometric

2   data.

1   8.   The method of claim 1, wherein the authentication data is personal

2   data selected from among the following: a password, a smart card, and another

3   type of authentication card.

1   9.   The method of claim 1, wherein the client forwards the decrypted

2   one-time key to the server, thereby authenticating the user as the owner of the

3   private key.

1   10.   The method of claim 1, further comprising discarding the record ID

2   after returning the one-time key to the user.

1   11.   The method of claim 1, wherein the record ID and the encrypted

2   one-time key are further encrypted using a partner key, the method further

3   comprising decrypting the record ID and encrypted one-time key using the

4   partner key.

1   12.   The method of claim 11, wherein the partner key is a symmetric

2   key set up during registration of the partner.

1   13.   The method of claim 11, wherein the partner key is a private key of

2   the authentication server.

1   14.   A method of using a third party authentication server to

2   authenticate a user to a server, the method comprising:

3   looking up a record ID associated with the user;

4   generating a one-time key and encrypting the one-time key with a public

5   key of the user, and sending the encrypted one-time key and the record ID to the

6   user;

7   receiving authentication data, the authentication data being the decrypted

8   one-time key; and

9   permitting access to the server.

1   15.   The method of claim 14, comprising:

2   determining an authentication policy associated with the user; and

3   verifying that the authentication policy has been satisfied, prior to

4   permitting access to the server.

1   16.   The method of claim 15, wherein verifying that the authentication

2   policy has been satisfied comprises:

3   determining if the server should verify additional data; and

4   if so, requesting additional data from the user prior to generating the one-

5   time key.

1   17.   A third-party authentication system comprising:

2   an authentication server to receive a record ID for a user, and a one-time

3   key generated by the server and encrypted with a user's public key by the server;

4   a comparison logic to receive user authentication data from the client and

5   comparing whether the user's authentication data matches the record ID; and

6   a decryption logic to decrypt the one-time key with a private key

7   associated with the validated record ID, and returning the decrypted one-time

8   key to the client.

1   18.   The system of claim 17, further comprising:

2   a policy validation logic to receive a policy from the server, and determine

3   if the policy has been fulfilled; and

4   the decryption logic to decrypt the one-time key only if the policy has

5   been fulfilled.

1   19.   The system of claim 17, further comprising:

2   a nonce generation logic to generate a nonce, the nonce to be included

3   with the user authentication data from the client; and

4   the comparison logic to verify that the user authentication data includes

5   the appropriate nonce.

1   20.   The system of claim 17, further comprising a client registration

2   logic to register the user, the client registration logic comprising:

3   a key generation logic to generate a random public key/private key pair

4   for the user;

5   a record ID generation logic to generate a random record ID for the user;

6   and

7   the client registration logic to associate user authentication data with the

8   private key and the record ID.

1   21.   The system of claim 18, further comprising:

2   the interface to send the record ID and the public key to the user.

1   22.   The system of claim 19, wherein the interface establish a secure

2   connection with the user, prior to receiving registration authentication data.

1   23.   The system of claim 17, wherein a web page presented by the

2   server to the client prompts the user to enter the authentication data to log in to

3   the server.

1   24.   The system of claim 23, wherein the client's authentication data is

2   automatically redirected to the authentication server.

1   25.   The system of claim 17, wherein the authentication data is

2   biometric data.

1   26.   The system of claim 17, wherein the authentication data is personal

2   data selected from among the following: a password, a smart card, and another

3   type of authentication card.

1   27.   The system of claim 17, wherein the client forwards the decrypted

2   one-time key to the server, thereby authenticating the user as the owner of the

3   private key.

1   28.   The system of claim 17, further comprising a security mechanism to

2   discard the record ID after returning the one-time key to the user.

1   29.   The system of claim 17, wherein the decryption logic further

2   decrypts the record ID and the encrypted one-time key with a partner key.

1   30.   The system of claim 29, wherein the partner key is a symmetric key

2   set up during registration of the partner.

1   31.   The system of claim 29, wherein the partner key is a private key of

2   the authentication server.